# EXHIBIT A-2 IDENTIFICATION OF PRIOR ART THAT ANTICIPATES AND/OR RENDERS OBVIOUS THE ASSERTED '661 CLAIMS

	CLAIMS PATENT L.R. 3-3(B)
ASSERTED CLAIM	IDENTITY OF PRIOR ART THAT ANTICIPATES AND/OR RENDERS OBVIOUS THE ASSERTED CLAIM
1. A cryptographic processing device for securely performing a cryptographic processing operation including a sequence of instructions in a manner recipient to	ANTICIPATION  The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following references:
discovery of a secret by external monitoring, comprising:	Griffin '294 Sci.crypt Postings
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a	Dunlavy '201 The claim is anticipated under 35 U.S.C. § 102 (e) by the following references:
portion of a message;	Ugon '833
<ul><li>(b) a source of unpredictable information;</li><li>(c) a processor;</li></ul>	<b>OBVIOUSNESS</b> The claim is rendered obvious under 35 U.S.C. §103 by the above listed references
(i) connected to said input interface for receiving and cryptographically processing said quantity,	individually or in combination with one or more of the following references:  Ugon '833
(ii) configured to use said unpredictable information to conceal a correlation between externally monitorable signals and said secret during said processing of said quantity by modifying said sequence; and	Sci.crypt Postings Dunlavy '201 Hoppe '894 Wakerly (1989)
(d) an output interface for outputting said cryptographically processed quantity to a	Schaumüller-Bichl (1987) ISO 7816

Porthiant thoras	11 14 221
reapient meteot.	ruther, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify.
	SUGGESTION OR MOTIVATION TO COMBINE Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 11 S C 8 103 as the claim.
	merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida
	Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally smalled to
	person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that
	in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic
	Thon, '922 fully anticipate the allege and the second of t
	explicitly, implicitly, or inherently. In the event that Ugon '833 does not fully anticipate the claim, it nevertheless renders the claim invalid as obvious. For example,
	Ugon '833 teaches all elements of the claim and provides motivation to combine them, e.g., at 3:59-4:8 (the disclosed improvements are designed for use in ST16XY cards); 1:14-19 (the disclosed improvements are intended to be implemented in
	microprocessors and microcomputers which require protection). In the alternative, Ugon '833, in combination with one or more of the above listed references, renders the claim invalid as obvious
	Similarly, each of Griffin '294, the Sci.crvpt Postings, and Dunlavy '201 fully
	anticipates the claim by disclosing each of the claimed elements either explicitly, in the alternative any of these references randers the claim
7 The domine of claims 1 minutes at 1	obvious, alone or in combination with any of the above listed references.
2. The device of claim 1 wherein said input	ANTICIPATION

interface and said output interface are the same element.

The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following reference:

Dunlavy '201

The claim is anticipated under 35 U.S.C. § 102 (e) by the following reference:

Ugon '833

### **OBVIOUSNESS**

The claim is rendered obvious by any of the references or combinations of references showing obviousness of claim 1.

Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify.

# SUGGESTION OR MOTIVATION TO COMBINE

merely sets forth a combination of existing elements with no change in their respective person of ordinary skill in the art; (2) the prior art references as understood by a person functions nor does the combination provide a new or different function. See Sakraida Initially, no suggestion or motivation to combine one or more of the references listed in the art that the disclosed components had been or could be used with cryptographic of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement above is required to render the claim obvious under 35 U.S.C. § 103 as the claim references listed above is provided by: (1) the knowledge generally available to a Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the components had been or could be used with cryptographic processing devices. processing devices; and/or (6) a suggestion in the reference that the disclosed

For example, ISO 7816 shows standard pin assignments, which include an I/O

	interface.
4 The daving of alain 1	Each of Ugon '833 and Dunlavy '201 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, either of these references renders the claim obvious, alone or in combination with any of the above listed references.
cryptographic processing operation includes transforming a message with the Data Encryption Standard (DES).	OBVIOUSNESS  The claim is rendered obvious under 35 U.S.C. §103 by one or more of the following references:
	Ugon '833 Sci.crypt Postings Griffin '294 Dunlavy '201
	individually or in combination with one or more of the following references:
	Ugon *833 Sci.crypt Postings Griffin *294
	Dunlavy '201 Menezes (1997)
	Makerly (1989) Rankl (1997)
	Hoppe '894 ISO 7816
	Schaumüller-Bichl (1987)
	Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify.
	SUGGESTION OR MOTIVATION TO COMBINE Initially, no suggestion or motivation to combine one or more of the references listed

	above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57,60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices.
	For example, FIPS PUB 46-2 (1993) describes the DES standard and suggests its use in certain microprocessors. Additionally, Menezes (1997) at 250 discusses DES as a well-known cryptographic algorithm.
5. A cryptographic processing device for	ANTICIPATION
securely performing a cryptographic	The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following
processing operation implementing a	references:
permutation in a manner resistant to	
discovery of a secret by external monitoring,	Sci.crypt Postings
comprising:	Lindholm '725
(a) an input interface for receiving a quantity	Van Eck 111/
to be cryptographically processed, said	OBVIOUSNESS
portion of a message;	The claim is rendered obvious under 25 11 & C & 102 hy and as more after fall
(b) a source of unpredictable information;	references:
(c) a processor:	Sci.crypt Postings
(i) connected to said input interface for	Ugon '833
receiving and cryptographically processing	Lindholm '725 Van Eck '117

said quantity,	Dunlavy '201
(ii) configured to use said unpredictable information to conceal a correlation between	individually or in combination with one or more of the following references:
externally monitorable signals and said secret during said processing of said quantity by randomizing the order of said	Sci.crypt Postings Ugon '833
permutation; and	Lindholm '725 Van Eck '117
(d) an output interface for outputting said cryptographically processed quantity to a	Dunlavy '201 Honne '894
recipient thereof.	Wakerly (1989) Rankl (1997)
	Schaumüller-Bichl (1987)
	FIPS Pub 46-2 (1993)
	Menezes (1997)
	Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify.
	SUGGESTION OR MOTIVATION TO COMBINE
	above is required to render the claim obvious under 35 U.S.C. § 103 as the claim
	merely sets forth a combination of existing elements with no change in their respective
	unctions nor does the combination provide a new or different function. See Sakraida v. Ag Pro. Inc., 425 U.S. 273, 282 (1976). Anderson's-Black Rock, Inc. v. Pavement
	Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit
	and/or implicit teaching, suggestion, or inference to combine one or more of the
	references using above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art. (2) the prior art references as understood by a person
	of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that
	each prior art reference involves similar problems; (5) the knowledge of those skilled
	in the art that the disclosed components had been or could be used with cryptographic
	processing devices; and/or (6) a suggestion in the reference that the disclosed

	components had been or could be used with cryptographic processing devices.
	For example, Menezes (1997) at 10 teaches that permutations are commonly used in cryptographic operations.
	Each of Lindholm '725, the Sci.crypt Postings, and Van Eck '117 fully anticipates the claim by disclosing all claim elements either explicitly or implicitly or under the doctrine of inherency. In the alternative, any of these references renders the claim obvious alone or in combination.
6. A cryptographic processing device implemented on a single microchip for	ANTICIPATION  The claim is anticipated under 35 H s. C. 8 102 (2) 23 4 4 5 H s. C. 102 (2) 2 4 5 H s. C. 102 (
securely performing a cryptographic processing operation in a manner resistant to	references:
	Fruhauf '053 Griffin '294
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	Sci.crypt Postings Lisimaque '039 Saltwick '243 Malek '467
(b) a source of unpredictable information;	The claim is anticipated under 35 U.S.C. § 102 (e) by the following references:
(c) a processor:	Ugon '833
(i) connected to said input interface for receiving and cryptographically processing said quantity,	<b>OBVIOUSNESS</b> The claim is rendered obvious under 35 U.S.C. §103 by one or more of the following
(ii) configured to use said unpredictable	references:
said microchip's power consumption and said processing of said quantity by	Ugon '833 Fruhauf '053
expending additional electricity in said microchip during said processing; and	Sci.crypt Postings
(d) an output interface for outputting said	Saltwick '243

Malek '467	Vall ECK 11 / Høivik '098	Dunlavy '201	Lindholm '725	Lindholm '713	individually or in combination with one or more of the following references:	Ugon '833	Fruhauf '053	Cuttin '294	Sci.crypt Postings	Lisimaque '039	Saltwick '243	Malek '467	Van Eck *117	Høivik '098	Dunlavy '201	Lindholm '725	Lindholm '713	Guthery (1998)	. Hoppe '894	ISO 7816	Wakerly (1989)	Rankl (1997)	Guillou (1986)	Schaumüller-Bichl (1987)	Further, Visa reserves the right to demonstrate invalidity using one or more of the	control is the second of the s	SUGGESTION OR MOTIVATION TO COMBINE Initially, no suggestion or motivation to combine one or many of the second	1) The references are the companies of the conferences listed
cryptographically processed quantity to a recipient thereof.																												

merely sets forth a combination of existing elements with no change in their respective person of ordinary skill in the art; (2) the prior art references as understood by a person functions nor does the combination provide a new or different function. See Sakraida in the art that the disclosed components had been or could be used with cryptographic of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement references listed above is provided by: (1) the knowledge generally available to a above is required to render the claim obvious under 35 U.S.C. § 103 as the claim Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the components had been or could be used with cryptographic processing devices. processing devices; and/or (6) a suggestion in the reference that the disclosed

(1997) (describing subscriber networks as a potential implementation of smartcards) with Griffin '294. Further, Guthery teaches that smartcards are frequently designed For example, one of ordinary skill in the art would be motivated to combine Rankl implementation on any type of computer, computer peripheral or other type of having single-chip processors. Dunlavy '201 suggests (e.g., at 8:13-19) its electronic device. Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either anticipate the claim, it nevertheless renders the claim invalid as obvious. For example, Ugon '833 teaches all elements of the claim and provides motivation to combine them, Ugon '833, in combination with one or more of the above listed references, renders the e.g., at 3:59-4:8 (the disclosed improvements are designed for use in ST16XY cards); microprocessors and microcomputers which require protection). In the alternative, explicitly, implicitly, or inherently. In the event that Ugon '833 does not fully 1:14-19 (the disclosed improvements are intended to be implemented in claim invalid as obvious.

Similarly, each of Fruhauf '053, Griffin '294, the Sci. crypt Postings, Lisimaque '039, claimed elements either explicitly, implicitly, or inherently. In the alternative, any of Saltwick '243, and Malek '467 fully anticipates the claim by disclosing each of the

	T		. The second				~~~~	·	· · · · · · · · · · · · · · · · · · ·			••
these references renders the claim obvious, alone or in combination with any of the above listed references.	ANTICIPATION The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following references:	Van Eck '117 Griffin '294 Sci.crypt Postings Lisimaque '039 Malek '467	The claim is anticipated under 35 U.S.C. § 102 (e) by the following references:	Ugon '833	<b>OBVIOUSNESS</b> The claim is rendered obvious under 35 U.S.C. §103 by one or more of the following references:	Ugon '833 Dunlavy '201 Van Eck '117	Sci.crypt Postings Griffin '294	Lisimaque '039 Malek '467	alone or in combination with one or more of the following references:	Ugon '833	Dunlavy '201	Sci. crypt Postings
	/. The device of claim 6 including program logic to activate said expending during said processing.											

Griffin '294
Lisimaque '039
Malek '467
Guthery (1998)
ISO 7816
Hoppe '894
Wakerly (1989)

Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify.

Schaumüller-Bichl (1987)

Guillou (1986)

### SUGGESTION OR MOTIVATION TO COMBINE

merely sets forth a combination of existing elements with no change in their respective person of ordinary skill in the art; (2) the prior art references as understood by a person functions nor does the combination provide a new or different function. See Sakraida Initially, no suggestion or motivation to combine one or more of the references listed each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that references listed above is provided by: (1) the knowledge generally available to a above is required to render the claim obvious under 35 U.S.C. § 103 as the claim Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the components had been or could be used with cryptographic processing devices. processing devices; and/or (6) a suggestion in the reference that the disclosed

references renders the claim obvious, alone or in combination with any of the above Each of Ugon '833, Van Eck '117, Griffin '294, the Sci.crypt Postings, Lisimaque elements either explicitly, implicitly, or inherently. In the alternative, any of these '039, and Malek '467 fully anticipates the claim by disclosing each of the claimed

	listed references
8. The device of claim 7 including	isted foldings,
(a) program logic implementing said source of unpredictable information; and	ANTICIPATION The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following references:
(b) program logic to transmit said unpredictable information to an additional power expending circuit contained in soid	Lisimaque '039 Malek '467
microchip.	The claim is anticipated under 35 U.S.C. § 102 (e) by the following references:
	Ugon '833
	<b>OBVIOUSNESS</b> The claim is rendered obvious under 35 U.S.C. §103 by one or more of the following references:
	Ugon '833 Dunlavy '201 Lisimaque '039 Malek '467
	individually or in combination with one or more of the following references:
	Ugon '833
	Dunlavy '201
	Lisimaque '0.39 Malek '467
	Guthery (1998)
	Hoppe '894
	ISO 7816
	Wakerly (1989)
	Rankl (1997)
	Guillou (1986)

	Schaumulier-Bichl (1987)
	Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify.
	SUGGESTION OR MOTIVATION TO COMBINE Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective
	v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the
	references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved: (4) the fact that
	each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices.
	Each of Ugon '833, Lisimaque '039, and Malek '467 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In
	the alternative, any of these references renders the claim obvious, alone or in combination with any of the above listed references.
9. A cryptographic processing device for securely performing a cryptographic	ANTICIPATION  The claim is anticipated under 35 U.S.C. & 102 (a) and/or (b) by the following
processing operation in a manner resistant to discovery of a secret by external monitoring.	references:
comprising:	Fruhauf '053
(a) an input interface for receiving a quantity	Lindholm '713 Malek '467
quantity being representative of at least a	Dunlavy '201 Griffin '294

portion of a message:	
(b) a source of unpredictable information;	The claim is anticipated under 35 U.S.C. § 102 (e) by the following references:
(c) a processor: (i) connected to said input interface for	Ugon '833 Wuidart '917
receiving and cryptographically processing said quantity,	OBVIOUSNESS The claim is rendered obvious under 35 U.S.C. §103 by the following references:
information to conceal a correlation between externally monitorable signals and said secret during said processing of said	Ugon '833 Wuidart '917 Fruhauf '053
(d) an output interface for outputting said cryptographically processed quantity to a recipient thereof;	Lindnoim 7/13 Malek '467 Dunlavy '201 Griffin '294
(e) a hardware-implemented noise production subunit connected to said source of unpredictable information and configured to expend unpredictable amounts of electricity based on the output of said source of unpredictable information; and (f) an activation controller, which may be activated by software contained in said device, to activate and deactivate said expending of unpredictable amounts of electricity.	undividually or in combination with one or more of the following references:  Ugon '833  Wuidart '917  Fruhauf '053  Lindholm '713  Malek '467  Dunlavy '201  Griffin '294  Hoppe '894  ISO 7816  Wakerly (1989)  Rankl (1997)
	Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the

merely sets forth a combination of existing elements with no change in their respective person of ordinary skill in the art; (2) the prior art references as understood by a person Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either anticipate the claim, it nevertheless renders the claim invalid as obvious. For example, Ugon '833 teaches all elements of the claim and provides motivation to combine them, Ugon '833, in combination with one or more of the above listed references, renders the functions nor does the combination provide a new or different function. See Sakraida in the art that the disclosed components had been or could be used with cryptographic Initially, no suggestion or motivation to combine one or more of the references listed v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled e.g., at 3:59-4:8 (the disclosed improvements are designed for use in ST16XY cards); Similarly, each of Fruhauf '053, Lindholm '713, Malek '467, Dunlavy '201, Griffin references renders the claim obvious, alone or in combination with any of the above '294 and Wuidart '917 fully anticipates the claim by disclosing each of the claimed microprocessors and microcomputers which require protection). In the alternative, elements either explicitly, implicitly, or inherently. In the alternative, any of these references listed above is provided by: (1) the knowledge generally available to a above is required to render the claim obvious under 35 U.S.C. § 103 as the claim Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the components had been or could be used with cryptographic processing devices. explicitly, implicitly, or inherently. In the event that Ugon '833 does not fully processing devices; and/or (6) a suggestion in the reference that the disclosed 1:14-19 (the disclosed improvements are intended to be implemented in references listed in Exhibit A-1, and any other art it may later identify. SUGGESTION OR MOTIVATION TO COMBINE claim invalid as obvious. **OBVIOUSNESS** isted references. 10. The device of claim 9 wherein said

Source of unnredictable information is a	
hardware-implemented random number	The ciaim is rendered obvious under 35 U.S.C. §103 by the following references:
generator, and wherein said noise production	Ugon '833
subunit includes a digital-to-analog	Wuidart '917
converter.	Lindholm '713
	Malek '467
	Dunlavy '201
	Griffin '294
	individually or in combination with one or more of the following references:
	Ugon '833
	Wuidart '917
	Lindholm '713
	Malek '467
	Dunlavy '201
	Griffin, '294
	JP10197610
	JP10084223
	JP62082702
	JP62260406
	Hoppe '894
	ISO 7816
	Wakerly (1989)
	Rankl (1997)
	Schaumüller-Bichl (1987)
	Further, Visa reserves the right to demonstrate invalidity using one or more of the
	references listed in Exhibit A-1, and any other art it may later identify.
	SUGGESTION OR MOTIVATION TO COMBINE
	Initially, no suggestion or motivation to combine one or more of the references listed
	above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their accompanies.
STATES OF THE PROPERTY OF THE	Sometimes with the change in their respective

said power consumption.
(CO)
** X GUDI
Ugon 833

	Wuidart '917	OBV The c	Ugon '833 Wuidart '917	Griffin '294	Sci.crypt Postings Fruhauf '053	Sprunk '402	Lisimaque '039	Kolbert '057	Lindholm '725	Meyr '962	Nossen '423	Lindholm '713		Malek '467	Van Eck '117	Dunlavy '201	Høivik '098	individually or in combination with one or more of the following references:	Ugon '833	Wuidart '917	Griffin '294	Sci.crypt Postings		Sprunk '402	Lisimaque '039	Kolbert '057	Indhoir
--	--------------	--------------	---------------------------	--------------	------------------------------------	-------------	----------------	--------------	---------------	-----------	-------------	---------------	--	------------	--------------	--------------	-------------	--	-----------	--------------	--------------	--------------------	--	-------------	----------------	--------------	---------

Nossen '423 Lindholm '713 Saltwick '243 Malek '467 Van Eck '117 Dunlavy '201 Høivik '098 Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997)

Meyr ,962

Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify.

# SUGGESTION OR MOTIVATION TO COMBINE

merely sets forth a combination of existing elements with no change in their respective person of ordinary skill in the art; (2) the prior art references as understood by a person functions nor does the combination provide a new or different function. See Sakraida in the art that the disclosed components had been or could be used with cryptographic Initially, no suggestion or motivation to combine one or more of the references listed v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled references listed above is provided by: (1) the knowledge generally available to a above is required to render the claim obvious under 35 U.S.C. § 103 as the claim Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the components had been or could be used with cryptographic processing devices. processing devices; and/or (6) a suggestion in the reference that the disclosed

Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either

	explicitly, implicitly, or inherently. In the event that Ugon '833 does not fully anticipate the claim, it nevertheless renders the claim invalid as obvious. For example, Ugon '833 teaches all elements of the claim and provides motivation to combine them, e.g., at 3:59-4:8 (the disclosed improvements are designed for use in ST16XY cards);
	microprocessors and microcomputers which require protection). In the alternative, Ugon '833, in combination with one or more of the above listed references, renders the claim invalid as obvious.
	Similarly, each of Griffin '294, the Sci.crypt Postings, Fruhauf '053, Sprunk '402, Lisimaque '039, Kolbert '057, Lindholm '725, Meyr '962, Nossen '423, Lindholm '713, Saltwick '243, Malek '467 Van Eck '117 Dunlawy '201 Ecci.ii, '909
	Wuidart '917 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, any of these references renders the claim obvious, alone or in combination with any of the claim obvious.
1) The daving of plain 11	references.
noise production system comprises:	ANTICIPATION  The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following
(a) a source of randomness for generating initial noise having a random characteristic:	references:
(b) a noise processing module for improving the random characteristic of said initial	Griffin '294 Fruhauf '053 Lindholm '725
noise; and	Lindholm '713 Saltwick '243
vary said power consumption based on an output of said noise processing module.	Malek '467 Høivik '098
	The claim is anticipated under 35 U.S.C. § 102 (e) by the following references:
	Ugon '833 Wuidart '917
	OBVIOUSNESS

Initially, no suggestion or motivation to combine one or more of the references listed The claim is rendered obvious under 35 U.S.C. §103 by the following references: Further, Visa reserves the right to demonstrate invalidity using one or more of the individually or in combination with one or more of the following references: references listed in Exhibit A-1, and any other art it may later identify. SUGGESTION OR MOTIVATION TO COMBINE Schaumüller-Bichl (1987) Wakerly (1989) Lindholm '725 Lindholm '713 Lindholm '725 Lindholm '713 Saltwick '243 Wuidart '917 Saltwick '243 Fruhauf '053 Wuidart '917 Malek '467 Høivik '098 Rankl (1997) Griffin '294 Fruhauf '053 Malek '467 Høivik '098 Griffin '294 Hoppe '894 Ugon '833 Ugon '833 ISO 7816

13. The device of claim 12 wherein said noise production system is connected to said processor and is selectively operable under
***************************************

The claim is rendered obvious under 35 U.S.C. §103 by the following references:

Ugon '833

Wuidart '917

Griffin '294 Fruhauf '053

Lindholm '713

Lindholm '713 Malek '467 individually or in combination with one or more of the following references:

Ugon \*833

Wuidart '917

Griffin '294 Fruhauf '053

Findholm '713

Malek '467

Hoppe '894

ISO 7816 Wakerly (1989)

wakeriy (1989) Ranki (1997)

Schaumüller-Bichl (1987)

Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify.

## SUGGESTION OR MOTIVATION TO COMBINE

merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida Initially, no suggestion or motivation to combine one or more of the references listed v. Ag Pro. Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement above is required to render the claim obvious under 35 U.S.C. § 103 as the claim Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the

	references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices.
	Each of Ugon '833, Griffin '294, Lindholm '713, Malek '467, and Wuidart '917 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, any of these references renders the claim obvious, alone or in combination with any of the above listed references.
14. A cryptographic processing device for	ANTICIPATION
processing operation in a manner resistant to	The chalm is anticipated under 35 U.S.C. § 102 (e) by the following references:
nitorin	Ugon '833
of said device's power consumption, comprising:	OBVIOUSNESS
(a) an input/output interface for receiving	The claim is rendered obvious under 35 U.S.C. §103 by the following references:
data to be cryptographically processed, said data being representative of at least a portion of a message;	Ugon '833 Wuidart '917
(b) an oscillator generating a first clock sional:	individually or in combination with one or more of the following references:
(c) an innut interface for receiving a variable	Ugon '833
amount of power, said power consumption	Sprunk '402
varying measurably during said performance of said operation;	Sci.crypt Postings Hoppe *894
(d) a source of unpredictable information;	ISO 7816 Wakerly (1989)
(e) a clock decorrelator coupled to said source of unpredictable information for	Rankl (1997)

generating a second clock signal from said first clock signal using said unpredictable	Schaumüller-Bichl (1987)
information, such that said second clock signal cannot be reliably predicted from said first clock signal; and	Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify.
(f) a processor:	SUGGESTION OR MOTIVATION TO COMBINE
(i) clocked by said second clock signal,	Initially, no suggestion or motivation to combine one or more of the references listed   above is required to render the claim obvious under 35118 C 8 103 m the plants
(ii) configured to cryptographically	merely sets forth a combination of existing elements with no change in their respective
processing said data, and	functions nor does the combination provide a new or different function. See Sakraida
(iii) configured to output said	Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit
input/output interface.	and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the browledge committee in the complexity of the
	person of ordinary skill in the art; (2) the prior art references as understood by a nerson
	of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that
	each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed comments had been also as that the disclosed comments had been also b
	processing devices; and/or (6) a suggestion in the reference that the disclosed
	components had been or could be used with cryptographic processing devices.
	Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either
	explicitly, implicitly, or inherently. In the event that Ugon '833 does not fully
	anticipate the claim, it nevertheless renders the claim invalid as obvious. For example,
	Ogon 633 leaches all elements of the claim and provides motivation to combine them,
	e.8., at 3.32-4.0 (tile disclosed improvements are designed for use in S116XY cards);
	microprocessors and microcomputers which require protection) In the attention
	Ugon '833, in combination with one or more of the above listed references renders the
	claim invalid as obvious.
15. A cryptographic processing device for	ANTICIPATION
securely performing a cryptographic	The claim is anticipated under 35 U.S.C. § 102 (e) by the following references:
processing operation in a manner resistant to	
discovery of a secret by external monitoring	

of said device's power consumption.	
of said device's	comprising:

- data being representative of at least a portion data to be cryptographically processed, said (a) an input/output interface for receiving of a message;
- (b) an input interface for receiving an external clock signal;
- (c) an input interface for receiving a variable varying measurably during said performance amount of power, said power consumption of said operation;
- (d) a source of unpredictable information;
- generating an internal clock signal from said predicted from said external clock signal; unpredictable information, such that said source of unpredictable information for (e) a clock decorrelator coupled to said internal clock signal cannot be reliably external clock signal using said

#### (f) a processor:

- (i) clocked by said internal clock signal,
- (ii) configured to cryptographically processing said data, and
- cryptographically processed data using said (iii) configured to output said input/output interface.

#### Ugon \*833

### **OBVIOUSNESS**

The claim is rendered obvious under 35 U.S.C. §103 by the following references:

Wuidart '917 Ugon '833

individually or in combination with one or more of the following references:

Ugon '833

Wuidart '917 Sprunk '402

Sci.crypt Postings

Hoppe '894

ISO 7816

Wakerly (1989)

Schaumüller-Bichl (1987) Rankl (1997)

Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify.

# SUGGESTION OR MOTIVATION TO COMBINE

merely sets forth a combination of existing elements with no change in their respective person of ordinary skill in the art; (2) the prior art references as understood by a person functions nor does the combination provide a new or different function. See Sakraida Initially, no suggestion or motivation to combine one or more of the references listed of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement references listed above is provided by: (1) the knowledge generally available to a above is required to render the claim obvious under 35 U.S.C. § 103 as the claim Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the

	references listed in Exhibit A-1, and any other art it may later identify.
	SUGGESTION OR MOTIVATION TO COMBINE  Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices.
	The motivation to use an external signal to generate an internal signal may be found, for example, in Sprunk '402 at, e.g., 1:52-54 (random signal to generate clock eliminates the ability to predict the clock even if observable) and/or Sci.crypt Postings at, e.g. posting by Jim Bell, December 24, 1995 (using pseudorandomly varied oscillator would make resulting computer harder to bug). Further, Rankl (1997) at 44 and 264 teaches that smart card processors require an external clock signal.
17. The device of claim 15 wherein said source of unpredictable information comprises a hardware random number	ANTICIPATION The claim is anticipated under 35 U.S.C. § 102 (e) by the following references:
generator.	Ugon '833
	<b>OBVIOUSNESS</b> The claim is rendered obvious under 35 U.S.C. §103 by the following references:
	Ugon '833

Wuidart '917

individually or in combination with one or more of the following references:

Wuidart '917 Ugon '833

Sci.crypt Postings Sprunk '402

Hoppe '894 1SO 7816

Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987)

Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify,

# SUGGESTION OR MOTIVATION TO COMBINE

merely sets forth a combination of existing elements with no change in their respective person of ordinary skill in the art; (2) the prior art references as understood by a person functions nor does the combination provide a new or different function. See Sakraida in the art that the disclosed components had been or could be used with cryptographic Initially, no suggestion or motivation to combine one or more of the references listed v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled above is required to render the claim obvious under 35 U.S.C. § 103 as the claim references listed above is provided by: (1) the knowledge generally available to a Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the components had been or could be used with cryptographic processing devices. processing devices; and/or (6) a suggestion in the reference that the disclosed

Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either

18. The device of claim 15 further comprising a monitor for detecting a clock fault in said external clock signal and preventing said processor from processing said quantity if said clock fault is detected.	explicitly, implicitly, or inherently. In the alternative, Ugon '833, alone or in combination with one or more of the above listed references, renders the claim invalid as obvious.  OBVIOUSNESS  The claim is rendered obvious under 35 U.S.C. §103 by the following references: Ugon '833  Wuidart '917  individually or in combination with one or more of the following references: Ugon '833  Wuidart '917  Sprunk '402  Sci.crypt Postings Griffin '294  Hoppe '894  ISO 7816  Wakerly (1987)  Rankl (1997)  Schaumüller-Bichl (1987)  Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify.  SUGGESTION OR MOTIVATION TO COMBINE  Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim morely sets forth a combination provide a new or different function. See Sakraida in An Prof. 17.5 272, 2021 020. 103. 103. 103. 103. 103. 103. 103. 10
	Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a

	person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices.
19 The device of claim 15 with	The motivation to a fault monitor as claimed is found, for example, in Griffin '294 at 2:30-36 and generally at 3:37-5:26.
clock decorrelator is selectively operable under the control of said processor.	ANTICIPATION The claim is anticipated under 35 U.S.C. § 102 (e) by the following references:
	Ugon *833
	<b>OBVIOUSNESS</b> The claim is rendered obvious under 35 U.S.C. §103 by the following references:
	Ugon '833 Wuidart '917
	individually or in combination with one or more of the following references:
	Ugon '833 Windort '017
	Sprunk '402
	Sci.crypt Postings
	Hoppe '894
	Wakerly (1989)
	Rankl (1997)
	Schaumüller-Bichl (1987)
	Further, Visa reserves the right to demonstrate invalidity using one or more of the

	references listed in Exhibit A-1, and any other art it may later identify.	SUGGESTION OR MOTIVATION TO COMBINE  Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro. Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices.	Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, Ugon '833, alone or in combination with one or more of the above listed references, renders the claim invalid as obvious.	clock decorrelator is selectively operable such that said clock decorrelator is disabled	when data is being transferred across said input/output interface and enabled during said cryptographic processing operation.  OBVIOUSNESS  The claim is rendered obvious under 35 11 S C 8103 by the following references.	Ugon '833
--	--	---	--	--	---	-----------

individually or in combination with one or more of the following references:

Ugon '833

Wuidart '917

Sci.crypt Postings Sprunk, 402

Lindholm '725

Hoppe '894

(SO 7816

Wakerly (1989)

Schaumüller-Bichl (1987) Rankl (1997)

Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify.

## SUGGESTION OR MOTIVATION TO COMBINE

merely sets forth a combination of existing elements with no change in their respective person of ordinary skill in the art; (2) the prior art references as understood by a person functions nor does the combination provide a new or different function. See Sakraida in the art that the disclosed components had been or could be used with cryptographic Initially, no suggestion or motivation to combine one or more of the references listed of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement above is required to render the claim obvious under 35 U.S.C. § 103 as the claim references listed above is provided by: (1) the knowledge generally available to a Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the components had been or could be used with cryptographic processing devices. processing devices; and/or (6) a suggestion in the reference that the disclosed

Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, Ugon '833, alone or in

21. The device of claim 15 further comprising a noise production system connected to said processor for introducing noise into said measurement of the power consumption by consuming a random amount of power during said cryptographic prosing operation.	combination with one or more of the above listed references, renders the claim invalid as obvious.  ANTICIPATION  The claim is anticipated under 35 U.S.C. § 102 (e) by the following references: Ugon '833  Wuidart '917  Ugon '833  Wuidart '917  Sprunk '402  Sci.crypt Postings  Hoppe '894  ISO 7816  Wakerly (1989)  Rankl (1997)  Schaumüller-Bichl (1987)
	ruther, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify.
	SUGGESTION OR MOTIVATION TO COMBINE Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective

functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that cach prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices.		The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following references:	Griffin '294 Sci.crypt Postings Dunlavy '201	The claim is anticipated under 35 U.S.C. § 102 (e) by the following references: Ugon '833	OBVIOUSNESS  The claim is rendered obvious under 35 U.S.C. §103 by the above listed references, individually or in combination with one or more of the following references:	Ugon '833 Griffin '294
	22. A device according to claims 1 4 7	11, 14, 15, or 20 wherein said device comprises a smartcard.				

merely sets forth a combination of existing elements with no change in their respective person of ordinary skill in the art; (2) the prior art references as understood by a person functions nor does the combination provide a new or different function. See Sakraida in the art that the disclosed components had been or could be used with cryptographic Initially, no suggestion or motivation to combine one or more of the references listed v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled implicitly, or inherently. In the alternative, any of these references renders the claim Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed above is provided by: (1) the knowledge generally available to a above is required to render the claim obvious under 35 U.S.C. § 103 as the claim Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit anticipates the claim by disclosing each of the claimed elements either explicitly, and/or implicit teaching, suggestion, or inference to combine one or more of the Each of Ugon '833, Griffin '294, the Sci.crypt Postings, and Dunlavy '201 fully components had been or could be used with cryptographic processing devices. The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following processing devices; and/or (6) a suggestion in the reference that the disclosed obvious, alone or in combination with any of the above listed references. references listed in Exhibit A-1, and any other art it may later identify. SUGGESTION OR MOTIVATION TO COMBINE Schaumüller-Bichl (1987) Sci.crypt Postings Wakerly (1989) Dunlavy '201 Rankl (1997) Hoppe '894 ANTICIPATION SO 7816 manner resistant to discovery of a secret cryptographic processing operation in a 23. A method of securely performing a

within a cryptographic processing device by rexternal monitoring, comprising:

- (a) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;
- (b) generating unpredictable information;
- (c) cryptographically processing said quantity, including using said unpredictable information while processing said quantity to conceal a correlation between externally monitorable signals and said secret by selecting between:
- (c)(1) performing a computation and incorporating the result of said computation in said cryptographic processing, and
- (c)(2) performing a computation whose output is not incorporated in said cryptographic processing; and
- (d) outputting said cryptographically processed quantity to a recipient thereof.

reference;

Dunlavy '201

The claim is anticipated under 35 U.S.C. § 102 (e) by the following reference:

Ugon '833

#### **OBVIOUSNESS**

The claim is rendered obvious by any of the references or combinations of references showing obviousness of claim 1.

Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify.

# SUGGESTION OR MOTIVATION TO COMBINE

Initially, no suggestion or motivation to combine one or more of the references listed See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an the references listed above is provided by: (1) the knowledge generally available to a explicit and/or implicit teaching, suggestion, or inference to combine one or more of those skilled in the art that the disclosed components had been or could be used with person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the respective functions nor does the combination provide a new or different function. cryptographic processing devices; and/or (6) a suggestion in the reference that the above is required to render the claim obvious under 35 U.S.C. § 103 as the claim fact that each prior art reference involves similar problems; (5) the knowledge of person of ordinary skill in the art; (2) the prior art references as understood by a disclosed components had been or could be used with cryptographic processing merely sets forth a combination of existing elements with no change in their

For example, ISO 7816 shows standard pin assignments, which include

	an I/O interface.
24. The method of claim 23 where said	Each of Ugon '833 and Dunlavy '201 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, either of these references renders the claim obvious, alone or in combination with any of the above listed references.
selecting is performed in software.	The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following references:
	Griffin '294 Sci.crypt Postings Malek '467 Van Eck '117
	The claim is anticipated under 35 U.S.C. § 102 (e) by the following references: Ugon '833
	<b>OBVIOUSNESS</b> The claim is rendered obvious under 35 U.S.C. §103 by the following references:
	Ugon '833 Griffin '294 Sci.crypt Postings Malek '467 Van Eck '117
	individually or in combination with one or more of the following references:
	Ugon '833 Griffin '294
	Sci.crypt Postings Malek '467

	Van Eck '117
	Hoppe *894
	11/21/21/21/21/21/21/21/21/21/21/21/21/2
	wakerly (1989)
	Kanki (1997)
	Schaumüller-Bichl (1987)
	Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify.
	SUGGESTION OR MOTIVATION TO COMBINE
	Initially, no suggestion or motivation to combine one or more of the references listed
	above is required to render the claim obvious under 35 U.S.C. § 103 as the claim
	functions nor does the combination provide a new or different functions for does the combination provide a new or different function.
	v. Ag Pro, Inc., 425 U.S. 273, 282 (1976): Anderson's-Black Rock Inc. v. Pavement
	Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit
	and/or implicit teaching, suggestion, or inference to combine one or more of the
	references listed above is provided by: (1) the knowledge generally available to a
	person of ordinary skill in the art; (2) the prior art references as understood by a person
	of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that
	each prior art reference involves similar problems; (5) the knowledge of those skilled
	in the art that the disclosed methods had been or could be used with cryptographic
	processing methods; and/or (6) a suggestion in the reference that the disclosed methods
	nad ocen of could be used with cryptographic processing methods.
	Each of Ugon '833, Griffin '294, the Sci.crypt Postings, Malek '467 and Van Eck '117
	fully anticipates the claim by disclosing each of the claimed elements either explicitly,
	implicitly, or inherently. In the alternative, any of these references renders the claim
25 The mother of alone 22 when	Arthory, arous of the computation with any of the above listed references.
25. The inctiou of ciain 25 where said selecting is performed in hardware on an integrated circuit including a	The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following references:

microprocessor.	Griffin '294
	Malek '467
	Van Eck '117
	The claim is anticipated under 35 U.S.C. § 102 (e) by the following references:
	Ugon '833
	OBVIOUSNESS The claim is rendered obvious under 35 U.S.C. §103 by the following references:
	Ugon '833 Griffin '294
	Sci.crypt Postings
	Malek '467
	Van Eck '117
	individually or in combination with one or more of the following references:
	Ugon '833
	Griffin '294
	Sci.crypt Postings
	Malek 46/
	Van Eck '117
	Hoppe '894
	150 7816
	Wakerly (1989)
	Ranki (1997)
	Schaumtiller-Bichl (1987)
	Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify.
	ייים היין כחובי מיין וועם ומכון ותכוווון אי

SUGGESTION OR MOTIVATION TO COMBINE
initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim
merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function.
v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement
<u>Salvage Co.</u> , 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching suggestion or information.
references listed above is provided by: (1) the knowledge generally available to a
person of ordinary skill in the art; (2) the prior art references as understood by a person
each prior art reference involves similar problems: (5) the knowledge of those skilled
in the art that the disclosed methods had been or could be used with cryptographic
processing methods, and/or (6) a suggestion in the reference that the disclosed methods had been or could be used with grantgoorneling and the supplementation of the supplementation o
mes even of court of used with cryptograpine processing methods.
Each of Ugon '833, Griffin '294, the Sci.crypt Postings, Malek '467 and Van Eck '117
fully anticipates the claim by disclosing each of the claimed elements either explicitly,
Implicitly, or inherently. In the alternative, any of these references renders the claim obvious, alone or in combination with any of the above listed references.
ANTICIPATION
The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following
references:
(
Griffin '294
Van Eck '117 Hoivik '098
The claim is anticipated under 35 U.S.C. § 102 (e) by the following reference:
Ugon '833
OBVIOUSNESS

information while processing said quantity to conceal a correlation between externally monitorable signals and said secret by selecting a code process from a plurality of code processes, where said selected code process is involved in said cryptographic processing, but where the value of said outputted quantity is independent of which of said code processes was selected; and (d) outputting said cryptographically

The claim is rendered obvious under 35 U.S.C. §103 by the following references: Ugon '833

Griffin '294 Van Eck '117 Hoivik '098 individually or in combination with one or more of the following references:

Ugon '833 Griffin '294 Van Eck '117 Hoivik '098 Sci.crypt Postings Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987)

processed quantity to a recipient thereof.

Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify.

#### SUGGESTION OR MOTIVATION TO COMBINE

merely sets forth a combination of existing elements with no change in their respective person of ordinary skill in the art; (2) the prior art references as understood by a person functions nor does the combination provide a new or different function. See Sakraida Initially, no suggestion or motivation to combine one or more of the references listed v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that references listed above is provided by: (1) the knowledge generally available to a above is required to render the claim obvious under 35 U.S.C. § 103 as the claim Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the

Section.

·^			<del></del>				
each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed methods had been or could be used with cryptographic processing methods; and/or (6) a suggestion in the reference that the disclosed methods had been or could be used with cryptographic processing methods.	Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the event that Ugon '833 does not fully anticipate the claim, it nevertheless renders the claim invalid as obvious. For example, Ugon '833 teaches all elements of the claim and provides motivation to combine them, e.g., at 3:59-4:8 (the disclosed improvements are designed for use in ST16XY cards); 1:14-19 (the disclosed improvements are intended to be implemented in microprocessors and microcomputers which require protection). In the alternative, Ugon '833, in combination with one or more of the above listed references, renders the claim invalid as obvious.	Similarly, each of Griffin '294, Van Eck '117, and Hoivik '098 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, any of these references renders the claim obvious, alone or in combination with any of the above listed references.	ANTICIPATION The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following references:	Griffin '294 Dunlavy '201 Lindholm '713	Sci. crypt Postings  The claim is anticipated under 35 U.S.C. § 102 (e) by the following reference:	Ugon '833	OBVIOUSNESS
		2 - 2 - 2 - 2 - 2 - 2 - 2 - 2 - 2 - 2 -	cryptographic processing operation including a sequence of instructions in a manner resistant to discovery of a secret	within a cryptographic processing device by external monitoring, comprising:  (a) receiving a quantity to be	cryptographically processed, said quantity being representative of at least a portion of a message;	(b) generating unpredictable information;	(c) using said unpredictable information while processing said quantity to conceal a

	ı
correlation between externally monitorable	`
signals and said secret by using said	
unpredictable information to modify said	
sequence; and	

(d) outputting said cryptographically processed quantity to a recipient thereof.

Sci.crypt Postings

The claim is rendered obvious under 35 U.S.C. §103 by the following references:

Griffin '294

Dunlavy '201

Lindholm '713

Ugon '833 individually or in combination with one or more of the following references:

Griffin '294 Dunlavy '201

Lindholm '713

Sci.crypt Postings

Ugon '833 Hoppe '894

ISO 7816

Wakerly (1989)

Rankl (1997) Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify.

# SUGGESTION OR MOTIVATION TO COMBINE

merely sets forth a combination of existing elements with no change in their respective person of ordinary skill in the art; (2) the prior art references as understood by a person functions nor does the combination provide a new or different function. See Sakraida Initially, no suggestion or motivation to combine one or more of the references listed v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement references listed above is provided by: (1) the knowledge generally available to a above is required to render the claim obvious under 35 U.S.C. § 103 as the claim Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the

	of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed methods had been or could be used with cryptographic processing methods; and/or (6) a suggestion in the reference that the disclosed methods had been or could be used with cryptographic processing methods.
·	Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the event that Ugon '833 does not fully anticipate the claim, it nevertheless renders the claim invalid as obvious. For example, Ugon '833 teaches all elements of the claim and provides motivation to combine them, e.g., at 3:59-4:8 (the disclosed improvements are designed for use in ST16XY cards); 1:14-19 (the disclosed improvements are intended to be implemented in microprocessors and microcomputers which require protection). In the alternative, Ugon '833, in combination with one or more of the above listed references, renders the claim invalid as obvious.
	Similarly, each of Griffin '294, Lindholm '713, Dunlavy '201, and the Sci.crypt Postings fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, any of these references renders the claim obvious, alone or in combination with any of the above listed references.
28. A method of securely performing a cryptographic processing operation implementing a permutation in a manner resistant to discovery of a secret within a	ANTICIPATION  The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following references:
cryptographic processing device by external monitoring, comprising:  (a) receiving a quantity to be	Sci.crypt Postings Lindholm '725 Van Eck '117
cryptographically processed, said quantity being representative of at least a portion of a	OBVIOUSNESS
message; (b) generating unpredictable information;	The claim is rendered obvious under 35 U.S.C. §103 by one or more of the following references:
(c) using said unpredictable information	Sci.crypt Postings

Ugon '833 Lindholm '725 Van Eck '117 Dunlavy '201	individually or in combination with one or more of the following references:	Sci.crypt Postings Ugon '833 Lindholm '725 Van Eck '117 Dunlavy '201 Hoppe '894 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) ISO 7816 FIPS Pub 46-2 (1993) Menezes (1997)	Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify.	SUGGESTION OR MOTIVATION TO COMBINE  Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida V. Ag Pro. Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that
while processing said quantity to conceal a correlation between externally monitorable signals and said secret by randomizing the order of said permutation; and	(d) outputting said cryptographically processed quantity to a recipient thereof.		14 E	STATE NOTE TO

each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed methods had been or could be used with cryptographic processing methods; and/or (6) a suggestion in the reference that the disclosed methods had been or could be used with cryptographic processing methods.	For example, Menezes (1997) at 10 teaches that permutations are commonly used in cryptographic operations.	Each of Van Eck '117, Lindholm '725, and the Sci.crypt Postings fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, any of these references renders the claim obvious, alone or in combination with any of the claim of the claim obvious, alone	ANTICIPATION	The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following	references:	Griffin '294	Sci.crypt Postings	Fruhauf '053	Sprink 402 Lisimanie '039	Kolbert '057	Lindholm '725	Meyr '962	Nossen '423	Saltwick '243	Malek '467	Van Eck '117	Dunlavy '201	NOTATION OF STREET	The claim is anticipated under 35 U.S.C. § 102 (e) by the following references:
			29. A method of securely performing a	Ctyptographic processing operation in a manner resistant to discovery of a good	within a cryptographic processing device hy	external monitoring of said device's power	consumption, comprising:	(a) receiving a variable amount of power,	said power consumption varying measurably	duling salu periormance of said operation;	(b) receiving a quantity to be	cryptographically processed, said quantity	ocing representative of at least a portion of a niessage;	(c) introducing noise into said magazine	of said power consumption while processing	said quantity; and	(d) outputting said cryptographically	processed quantity to a recipient thereof.	

				~~~~~	•		·····				******													
Ugon '833 Wuidart '917	<b>OBVIOUSNESS</b> The claim is rendered obvious under 35 U.S.C. §103 by the following references:	Ugon '833	Wuidart '917 Griffin '294	Sci.crypt Postings	Sprunk '402	Lisimaque '039	Kolbert '057	Meyr '962	Nossen '423	Lindholm '713	Saltwick '243	Malek '467	Van Eck '117	Dunlavy '201	Høivik '098	individually or in combination with one or more of the following references:	Ugon '833	Wuidart '917	Griffin '294	Sci.crypt Postings	Fruhauf '053	Sprunk '402	Lisimaque '039	Kolbert '057

Lindholm '725

Meyr '962
Nossen '423
Lindholm '713
Saltwick '243
Malek '467
Van Eck '117
Dunlavy '201
Høivik '098
Hoppe '894
ISO 7816
Wakerly (1989)
Rankl (1997)
Schaumüller-Bichl (1987)

Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify.

# SUGGESTION OR MOTIVATION TO COMBINE

merely sets forth a combination of existing elements with no change in their respective processing methods; and/or (6) a suggestion in the reference that the disclosed methods person of ordinary skill in the art; (2) the prior art references as understood by a person functions nor does the combination provide a new or different function. See Sakraida Initially, no suggestion or motivation to combine one or more of the references listed of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that v. Ag Pro. Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed methods had been or could be used with cryptographic references listed above is provided by: (1) the knowledge generally available to a above is required to render the claim obvious under 35 U.S.C. § 103 as the claim Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the nad been or could be used with cryptographic processing methods.

Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the event that Ugon '833 does not fully anticipate the claim, it nevertheless renders the claim invalid as obvious. For example, Ugon '833 teaches all elements of the claim and provides motivation to combine them, e.g., at 3:59-4:8 (the disclosed improvements are designed for use in ST16XY cards); 1:14-19 (the disclosed improvements are intended to be implemented in microprocessors and microcomputers which require protection). In the alternative, Ugon '833, in combination with one or more of the above listed references, renders the claim invalid as obvious.	Similarly, each of Griffin '294, the Sci.crypt Postings, Fruhauf '053, Sprunk '402, Lisimaque '039, Kolbert '057, Lindholm '725, Meyr '962, Nossen '423, Lindholm '713, Saltwick '243, Malek '467, Van Eck '117, Dunlavy '201, Høivik '098, and Wuidart '917 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, any of these references renders the claim obvious, alone or in combination with any of the above listed references.	ANTICIPATION  The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following references:	Crittin '294 Fruhauf '053 Lindholm '725 Lindholm '713 Saltwick '243 Malek '467 Høivik '098	The claim is anticipated under 35 U.S.C. § 102 (e) by the following references:	Ugon '833 Wuidart '917
		30. The method of claim 29 wherein said step of introducing noise comprises:  (a) generating initial noise having a random characteristic;	<ul><li>(b) improving the random characteristic of said initial noise; and</li><li>(c) varying said power consumption based on said improved initial noise.</li></ul>		

THE RESERVE THE PROPERTY OF TH	The second secon
	OBVIOUSNESS
	The claim is rendered obvious under 35 U.S.C. §103 by the following references:
	Ugon '833
	Wuidart '917
	Griffin '294
	Fruhauf '053
	Lindholm '725
	Lindholm '713
	Saltwick '243
	Malek '467
	Høivik '098
	individually or in combination with one or more of the following references:
	Ugon '833
	Wuidart '917
	Griffin '294
	Fruhauf '053
	Lindholm '725
	Lindholm '713
	Saltwick '243
	Malek '467
	Høivik '098
	Hoppe '894
	ISO 7816
	Wakerly (1989)
	Rankl (1997)
	Schaumüller-Bichl (1987)
	Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify.
· · · · · · · · · · · · · · · · · · ·	SUGGESTION OR MOTIVATION TO COMBINE

	Initially, no suggestion or motivation to combine one or more of the references listed
	above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with an obstage in their accompanies.
	functions nor does the combination provide a new or different function. See Sakraida
***	v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement
	and/or implicit teaching, suggestion, or inference to combine one or more of the
	references listed above is provided by: (1) the knowledge generally available to a
	of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that
	each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed methods had been or could be used unith countainship.
	processing methods; and/or (6) a suggestion in the reference that the disclosed methods
	had been or could be used with cryptographic processing methods.
	Each of Ugon '833, Griffin '294, Fruhauf '053, Lindholm '725, Lindholm '713,
4	Saltwick '243, Malek '467, Hoivik '098, and Wuidart '917 fully anticipates the claim
	In the alternative, any of these references renders the claim obvious, alone or in
	combination with any of the above listed references.
31. A method of securely performing a	ANTICIPATION
cryptographic processing operation in a	The claim is anticipated under 35 U.S.C. § 102 (e) by the following references:
manner resistant to discovery of a secret	
within a cryptographic processing device by external monitoring of said device's power	Ugon '833 Wuidart '917
consumption, comprising:	
(a) receiving a variable amount of power,	OBVIOUSNESS The claim is rendered obvious under 35 LLS C 8103 by the following references:
said power consumption varying measurably	the communication of the control of
during said performance of said operation;	Ugon '833
(b) generating a first clock signal;	Wuidart '917
(c) receiving data to be cryptographically	

processed, said data being representative of indivat least a portion of a message;

- (d) generating unpredictable information;
- (e) generating a second clock signal from said first clock signal using said unpredictable information, such that said second clock signal cannot be reliably predicted from said first clock signal;
- (f) processing said data using said second clock signal; and
- (g) outputting said cryptographically processed quantity to a recipient thereof.

individually or in combination with one or more of the following references:

Ugon '833 Wuidart '917

Sprunk '402 Sci.crypt Postings

Sci.crypt Fosting Hoppe \*894

ISO 7816

Wakerly (1989)

Rankl (1997) Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify.

### SUGGESTION OR MOTIVATION TO COMBINE

processing methods; and/or (6) a suggestion in the reference that the disclosed methods merely sets forth a combination of existing elements with no change in their respective person of ordinary skill in the art; (2) the prior art references as understood by a person functions nor does the combination provide a new or different function. See Sakraida Initially, no suggestion or motivation to combine one or more of the references listed each prior art reference involves similar problems; (5) the knowledge of those skilled of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement in the art that the disclosed methods had been or could be used with cryptographic references listed above is provided by: (1) the knowledge generally available to a above is required to render the claim obvious under 35 U.S.C. § 103 as the claim Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the had been or could be used with cryptographic processing methods. Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either anticipate the claim, it nevertheless renders the claim invalid as obvious. For example, explicitly, implicitly, or inherently. In the event that Ugon '833 does not fully

	Ugon '833 teaches all elements of the claim and provides motivation to combine them, e.g., at 3:59-4:8 (the disclosed improvements are designed for use in ST16XY cards); 1:14-19 (the disclosed improvements are intended to be implemented in microprocessors and microcomputers which require protection). In the alternative, Ugon '833, in combination with one or more of the above listed references, renders the claim invalid as obvious.
3 A method of one	Similarly, Wuidart '917 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, Wuidart '917 renders the claim obvious, alone or in combination with any of the above listed references.
cryptographic processing operation in a manner resistant to discovery of a secret	ANTICIPATION The claim is anticipated under 35 U.S.C. § 102 (e) by the following references:
within a cryptographic processing device by external monitoring of said device's power	Ugon '833
consumption, comprising:	OBVIOUSNESS The claim is rendered obvious under 35 11 8 C 8102 by the current
during said performance of said operation;	Ugon '833 Wuidart '917
(b) receiving an external clock signal;	individually or in combination with one or more of the following references;
processed, said data being representative of at least a portion of a message;	Ugon '833 Wuidart '917
(d) generating unpredictable information;	Sprunk '402
(e) generating an internal clock signal from said external clock signal using said	Sel. crypt Postings Hoppe '894 ISO 7816
unpredictable information, such that said external clock signal cannot be reliably	Wakerly (1989) Rankl (1997)
predicted from said internal clock signal;	Schaumüller-Bichl (1987)
(f) processing said data using said internal	

clock sinnal and	
(g) outputting said cryptographically	Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify.
processed quantity to a recipient thereof.	SUGGESTION OR MOTIVATION TO COMBINE
	Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 25 11 6 % 6 10.
	merely sets forth a combination of existing elements with no change in their respective
	unctions nor does the combination provide a new or different function. See Sakraida
	Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit
	and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge and it is a standard by: (1) the knowledge and it is the standard by: (1) the knowledge and it is the standard by: (1) the knowledge and it is the standard by: (1) the knowledge and it is the standard by: (1) the knowledge and it is the standard by: (1) the knowledge and it is the standard by: (1) the knowledge and it is the standard by: (1) the knowledge and it is the standard by: (1) the knowledge and it is the standard by: (2) the knowledge and it is the standard by: (3) the knowledge and it is the standard by: (3) the standard by: (4) the standard by: (5) the standard by: (5) the standard by: (6) the standard by: (7) the standard by: (7) the standard by: (7) the standard by: (8) the standard by: (
	person of ordinary skill in the art; (2) the prior art references as understood by a person
	of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that
	cacil prior art reference involves similar problems; (5) the knowledge of those skilled
	processing methods; and/or (6) a suggestion in the reference that the disclosed methods
	had been or could be used with cryptographic processing methods.
	Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either
	explicitly, implicitly, or inherently. In the event that Ugon '833 does not fully
	anticipate the claim, it nevertheless renders the claim invalid as obvious. For example, Ugon '833 teaches all elements of the claim and manifestations.
	e.g., at 3:59-4:8 (the disclosed improvements are designed for use in ST16XY carde).
	1:14-19 (the disclosed improvements are intended to be implemented in
	inicroprocessors and microcomputers which require protection). In the alternative,
	Ugon '833, in combination with one or more of the above listed references, renders the
33. The method of claim 32 wherein said	OBVIOLISNESS
step of generating said internal clock signal	The claim is rendered obvious under 35 11 S C 8103 by the following reference:
comprises a step of selecting a subset of the	Second and the contract of the
cycles of said external clock signal to use as	Ugon '833
said internal clock signal based on said	Wuldarf '91'

processing methods; and/or (6) a suggestion in the reference that the disclosed methods merely sets forth a combination of existing elements with no change in their respective person of ordinary skill in the art; (2) the prior art references as understood by a person functions nor does the combination provide a new or different function. See Sakraida unpredictable information may be found, for example, in Sprunk '402 at, e.g., 1:52-54 Initially, no suggestion or motivation to combine one or more of the references listed of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Further, Visa reserves the right to demonstrate invalidity using one or more of the in the art that the disclosed methods had been or could be used with cryptographic references listed above is provided by: (1) the knowledge generally available to a (random signal to generate clock eliminates the ability to predict the clock even if above is required to render the claim obvious under 35 U.S.C. § 103 as the claim Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the The motivation to use an external signal to generate an internal signal based on individually or in combination with one or more of the following references: references listed in Exhibit A-1, and any other art it may later identify. had been or could be used with cryptographic processing methods. SUGGESTION OR MOTIVATION TO COMBINE Schaumüller-Bichl (1987) Sci.crypt Postings Wakerly (1989) Wuidart '917 Sprunk '402 Rankl (1997) Hoppe '894 ISO 7816 unpredictable information.

ž

34. The method of claim 32 wherein said step of generating unpredictable information comprises a step of generating a random number.
--------------------------------------------------------------------------------------------------------------------------------------

7

<u>v. Ag Pro, Inc.</u> , 425 U.S. 273, 282 (1976); <u>Anderson's-Black Rock, Inc. v. Pavement and/or implicit teaching</u> , suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed methods had been or could be used with cryptographic processing methods; and/or (6) a suggestion in the reference that the disclosed methods had been or could be used with cryptographic processing methods.	Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, Ugon '833 renders the claim obvious, alone or in combination with any of the above listed references.	The claim is rendered obvious under 35 U.S.C. §103 by the following references:	Ugon `833 Wuidart '917	individually or in combination with one or more of the following references:	Ugon '833 Wujdart '917	Sprunk '402 Griffin '294	Sci.crypt Postings	Hoppe '894 ISO 7816	Wakerly (1989)	Schaumüller-Bichl (1987)	Further, Visa reserves the right to demonstrate invalidity using one or more of the
	35 The method of claim 32 firehar	comprising a step of monitoring for a clock fault in said external clock signal and a step	or preventing said processor from outputting said cryptographically processed quantity if said clock fault is detected.								

	references listed in Exhibit A-1, and any other art it may later identify.
	SUGGESTION OR MOTIVATION TO COMBINE  Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed methods had been or could be used with cryptographic processing methods; and/or (6) a suggestion in the reference that the disclosed methods had been or could be used with cryptographic processing methods.
	The motivation to implement a fault monitor as claimed is found, for example, in Griffin '294 at 2:30-36 and generally at 3:37-5:26.
36. The method of claim 32 further comprising a step of introducing noise into said measurement of the power	ANTICIPATION The claim is anticipated under 35 U.S.C. § 102 (e) by the following references:
consumption.	Ugon '833
	<b>OBVIOUSNESS</b> The claim is rendered obvious under 35 U.S.C. §103 by the following references:
	Ugon '833 Wuidart '917
	individually or in combination with one or more of the following references:
	Ugon '833

Wuidart '917
Sprunk '402
Sci.crypt Postings
Hoppe '894
ISO 7816
Wakerly (1989)
Rankl (1997)
Schaumüller-Bichl (1987)

Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify.

#### SUGGESTION OR MOTIVATION TO COMBINE

merely sets forth a combination of existing elements with no change in their respective processing methods; and/or (6) a suggestion in the reference that the disclosed methods person of ordinary skill in the art; (2) the prior art references as understood by a person functions nor does the combination provide a new or different function. See Sakraida Initially, no suggestion or motivation to combine one or more of the references listed of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed methods had been or could be used with cryptographic references listed above is provided by: (1) the knowledge generally available to a above is required to render the claim obvious under 35 U.S.C. § 103 as the claim Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the had been or could be used with cryptographic processing methods. Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, Ugon '833 renders the claim obvious, alone or in combination with any of the above listed references.